KOMBINASI LSB-RSA UNTUK PENINGKATAN IMPERCEPTIBILITY PADA KRIPTO-STEGANO GAMBAR RGB

Ajib Susanto[1], Ibnu Utomo Wahyu Mulyono[2]
[1,2]Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
e-mail: [1]ajib.susanto@dsn.dinus.ac.id, [2]ibnu.utomo.wm@dsn.dinus.ac.id

Abstrak

Steganografi adalah metode menyembunyikan pesan rahasia dalam objek sampul saat komunikasi terjadi antara pengirim dan penerima. Keamanan informasi rahasia atau penting selalu menjadi masalah utama dari masa lalu hingga saat ini. Itu selalu menjadi topik yang menarik bagi para peneliti untuk mengembangkan teknik aman untuk mengirim data tanpa mengungkapkannya kepada siapa pun selain penerima. Oleh karena itu dari hari ke hari para peneliti telah mengembangkan banyak teknik untuk memenuhi transfer data yang aman dan salah satunya adalah steganografi. Dalam makalah ini, telah diimplementasikan kombinasi steganografi gambar di dalam penyisipan file data atau pesan terenkripsi menggunakan LSB dengan algoritma RSA untuk memberikan keamanan lebih ke data serta metode penyembunyian data. Percobaan menggunakan 10 gambar ukuran 512x512 piksel dan pesan berupa teks dengan panjang 1024 bit dan 3027 bit sebagai perbandingan. Hasil akhir mendapatkan PSNR tertinggi yaitu 78 dB pada pesan 1024 bit.

***Kata Kunci**: LSB, RSA, gambar, stegano, kripto*

1. PENDAHULUAN

Kebutuhan dasar setiap area yang berkembang di dunia saat ini adalah komunikasi. Semua orang ingin menjaga informasi orang dalam agar rahasia dan aman. Kami menggunakan banyak jalur tidak aman dalam kehidupan sehari-hari untuk mentransfer dan berbagi informasi menggunakan internet atau melalui telepon, tetapi pada tingkat tertentu itu tidak aman. Steganografi dan Kriptografi adalah dua metode yang dapat digunakan untuk berbagi informasi secara tersembunyi. Kriptografi mencakup modifikasi pesan dengan cara yang bisa dicerna atau dienkripsi dalam bentuk yang dijaga oleh kunci enkripsi yang hanya diketahui oleh pengirim dan penerima dan tanpa menggunakan kunci enkripsi pesan tidak dapat diakses [1]. Namun dalam kriptografi, selalu jelas bagi orang perantara bahwa pesan tersebut dalam bentuk terenkripsi, sedangkan dalam steganografi, pesan rahasia dibuat untuk disembunyikan di gambar sampul sehingga tidak dapat lebih jelas bagi setiap orang perantara bahwa apakah ada pesan yang tersembunyi dalam informasi tersebut dibagikan [2]. Gambar sampul yang berisi pesan rahasia adalah proses dan kunci rahasia yang disediakan oleh pengirim. Gambar dianggap sebagai salah satu bentuk informasi yang paling banyak digunakan, revolusi internet dan penggunaan besar-besaran teknologi informasi memudahkan komunikasi dan dengan demikian membuat informasi menjadi lebih rapuh. Pertukaran data digital menimbulkan masalah keamanan, sehingga enkripsi menjadi lebih penting.

Berdasarkan kunci, kriptografi dapat di klasifikasikan ke dalam dua cabang yang dikenal sebagai simetris dan asimetris. Algoritma simetris yang paling dikenal adalah AES *(Advanced Encryption Standard)* [2], DES (*Data Encryption Standard)* [3] dan 3-DES. Teknik-teknik ini ekonomis dan relatif aman. Masalah terbesar dengan teknik ini adalah pertukaran dan penyimpanan kunci rahasia. Cabang kedua adalah *Asymmetric* (*public*) *key cryptosystem*, menggunakan algoritma yang sama untuk enkripsi dan dekripsi dengan sepasang kunci, publik dan privat, komputasi tidak mungkin untuk mendapatkan kunci privat dari kunci publik. Sistem asimetris seperti RSA *(Rivest, Shamir dan Adleman)* [1] membutuhkan penggunaan angka besar (lebih besar dari 512 bit) yang tidak sesuai untuk mengenkripsi gambar. Cabang kriptografi ini memiliki minat besar, karena menghilangkan masalah transfer kunci, namun waktu komputasinya relatif lama.

Steganografi juga bisa menjadi solusi untuk meningkatkan jumlah keamanan. Steganografi adalah teknik yang menyembunyikan data rahasia ke media sampul, sehingga tidak akan dapat mengekstraksi data rahasia [4]. Di antara semua metode yang terkenal, substitusi LSB *(Least Significant Bit)* [5], yang menyematkan data rahasia dengan mengganti k LSB suatu piksel dengan k bit-bit rahasia secara langsung.

Beberapa penelitian telah menguatkan hasil penyandian dan stegano dalam metode LSB, seperti yang dilakukan oleh Handoyo dkk dengan mengimplementasikan LSB-RSA16 bit pada cover gambar *grayscale* dan pesan juga berupa gambar *grayscale* [1]. Ukuran pesan yang digunakan yaitu 2562144 bit. Hasil akhir PSNR tertinggi yang diperoleh adalah 57 dB. Sedangkan Alamsyah [5], pada penelitiannya juga menggunakan LSB-RSA namun pada cover berupa gambar RGB dan pesan berupa teks 1360 bit. Hasil akhir diperoleh nilai PSNR tertinggi yaitu 69 dB. Penelitian lainnya dilakukan oleh Astuti dkk [6] dengan hanya menggunakan LSB pada mode *flipping* bit untuk melakukan steganografi pada gambar berwarna. Hasil akhir PSNR tertinggi yaitu 65.5438 dB. Nilai yang cukup tinggi pada flipping bit LSB di dapat dari pesan berupa gambar 256 × 128 piksel yang di sisipkan pada cover berukuran 512x 512 piksel. Modifikasi LSB menggunakan XOR pada MSB telah dilakukan oleh Astuti dkk [7]. Dalam penelitian tersebut digunakan gambar cover *grayscale* berukuran 256 x

256 piksel dengan gambar pesan berupa biner. Hasil eksperimen membuktikan nilai PSNR tertinggi adalah 56.035 dB.

Dalam makalah ini kami mengusulkan metode berdasarkan metode RSA dan LSB. Gambar dienkripsi menggunakan RSA dan disembunyikan di gambar menggunakan teknik LSB. Keuntungan utama dari kombinasi RSA-LSB adalah menghilangkan masalah transmisi kunci. Pendekatan yang disajikan lebih efisien dalam hal biaya komputasi dibandingkan dengan skema yang menggunakan enkripsi asimetris.

2. TINJAUAN PUSTAKA

2.1 LSB

Steganografi telah muncul sebagai area penelitian yang bersinar di mana berbagai metode telah diusulkan di beberapa media pembawa. Metode LSB memberikan ide steganografi yang sangat mendasar dengan cara yang mudah. Metode ini menyatakan bahwa bit pesan rahasia dapat ditempatkan dengan mengganti bit paling tidak signifikan dari piksel gambar [8]. Ini memungkinkan penyisipan 100% bit biner pesan dalam piksel suatu gambar dengan perubahan sangat kecil +1 atau −1 dalam nilai piksel [9]. Metode ini rentan terhadap serangan karena pesan hadir di LSB, dan dengan hanya memilih LSB, penyusup dapat mengakses data [1]. Kebisingan kuantisasi juga dapat menghancurkan data yang ada di LSB. LSB dapat dengan mudah diterjemahkan oleh penyusup dan juga tidak kebal terhadap teknik *noise* dan kompresi [10]. LSB hanya memungkinkan satu bit penyisipan data pesan di dalam piksel tertentu [11]. Misalkan string pesan yang dikirim melalui internet adalah 10010101, dan nilai piksel kontinu adalah sebagai berikut:

01101000 10101001 01101000 11110000 00011101 10000001 11110000 10101010

menjadi

01101001 10101000 01101000 11110001 00011100 10000001 11110000 10101011.

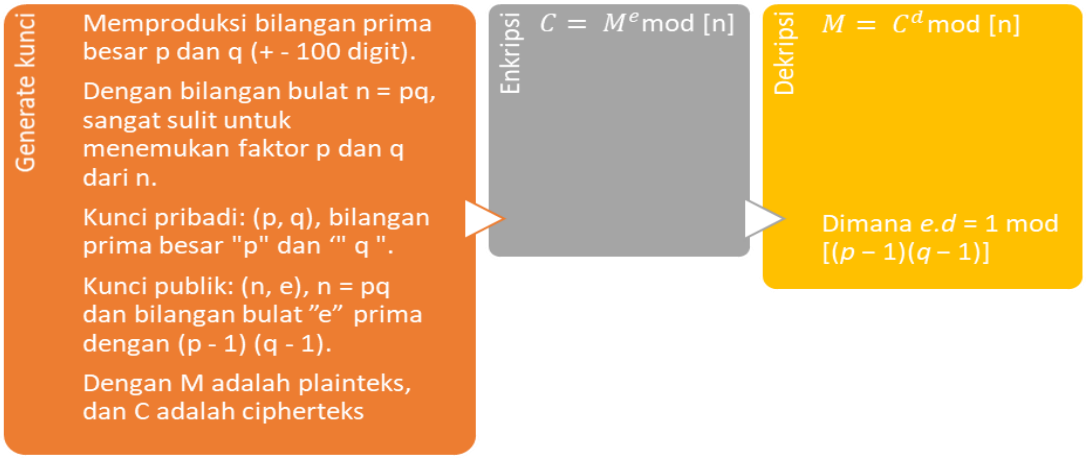
Metode ini rentan terhadap serangan karena pesan hadir di LSB, dan dengan hanya memilih LSB, penyusup dapat mengakses data. LSB dapat diimplementasikan berdasarkan bidang bit pertama dan kedua. Dalam metode ini, pada kombinasi bidang bit 1 dan 2 pesan disembunyikan. Hasil utama dari metode ini adalah bahwa kemungkinan penyisipan pesan di lokasi pseudorandom pada kesempatan pertama adalah 50%. Probabilitasnya adalah 50% ketika tidak perlu mengubah nilai piksel [12]. Probabilitasnya adalah 12,5% ketika perubahan dalam nilai piksel diperlukan. Pesan pada LSB dapat pula disembunyikan menggunakan bit 6, 7, dan 8 piksel dalam gambar skala abu-abu. Hasil utama dari metode ini adalah bahwa kemungkinan penyisipan pesan di lokasi *pseudorandom* pada kesempatan pertama adalah 85,93%. Peluang ketika pesan tidak diubah adalah 43.18%. Seperti yang ditunjukkan hasilnya, metode ini tidak memberikan tingkat penyisipan pesan 100%.

2.1 RSA

RSA diterbitkan pada tahun 1977 oleh Ron Rivest, Adi Shamir dan Leonard Adleman dari Massachusetts *Institute of Technology (MIT),* RSA didasarkan pada kesulitan memfaktorkan angka dalam jumlah yang besar [1] dengan bentuk *pseudocode* di bawah ini.

1. Begin.
2. m = the ASCII code of the plaintext.
3. c = the ASCII code of the ciphertext.
4. Choose two large prime numbers p and q (+100 digits).
5. Compute $\varphi(n) = (p - 1)(q - 1)$.
6. Compute $n = pq$
7. Choose any number $1 < e < \varphi(n)$ that is coprime to $\varphi(n)$.
8. Compute the value of d such that $(d * e) \bmod \varphi(n) = 1$.
9. Public key is (e, n).
10. Private key is (d, n).
11. The encryption of m is $c = m^e \bmod n$.
12. The decryption of c is $m = c^d \bmod n$.
13. End.

RSA menggunakan kunci yang sama untuk enkripsi dan dekripsi, membutuhkan sepasang kunci, kunci publik dan kunci privat, dengan tiga langkah utama yaitu menggenerate kunci, enkripsi dan dekripsi seperti Gambar 1 berikut ini:

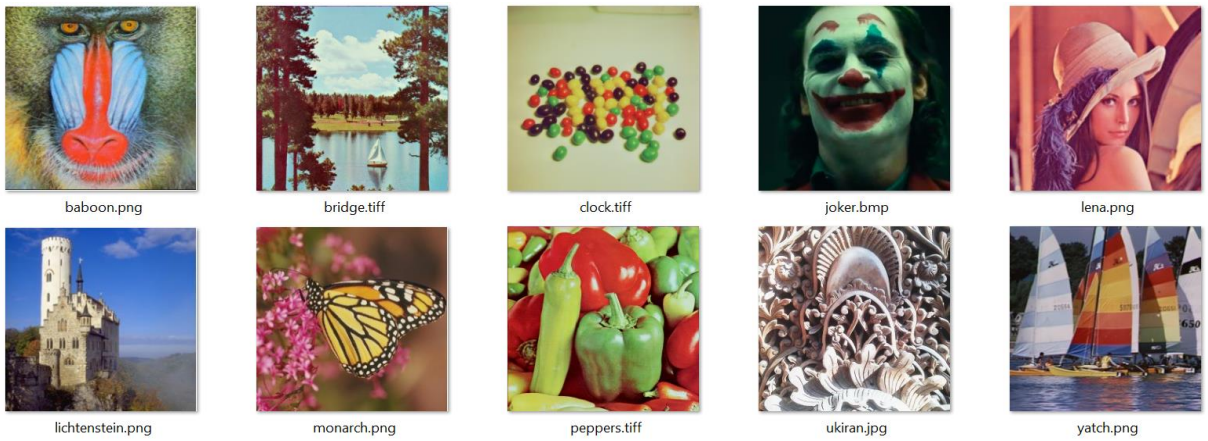


Gambar 1. Alur eksperimen dengan RSA

3. METODE PENELITIAN

3.1 Data Gathering

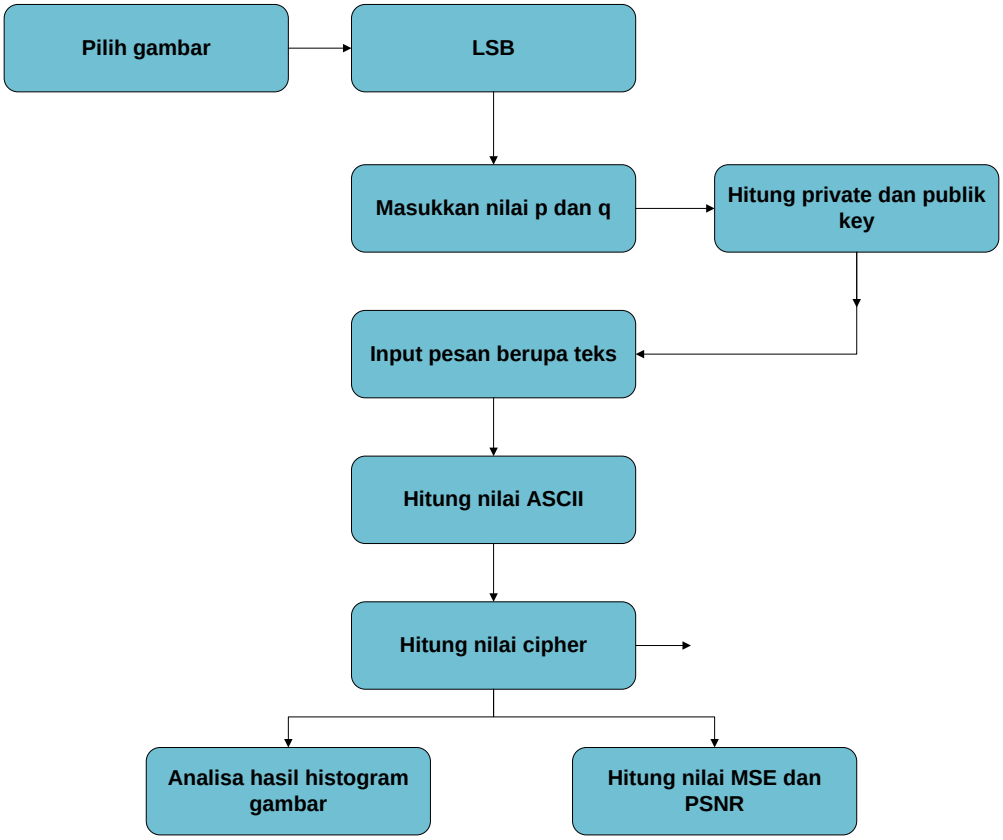
Penelitian tentang pemrosesan gambar terutama steganografi gambar terus berkembang hingga sekarang. Tetapi penelitian yang dikembangkan oleh penulis yang berbeda, terkadang menjadi sulit untuk ditiru atau dibandingkan, karena kurangnya penjelasan rinci tentang metode ini, atau karena penggunaan data yang tidak standar. Pemilihan dan pengumpulan data sangat penting dan menjadi salah satu penentu kualitas penelitian, oleh karena itu dalam penelitian ini, kami memilih gambar standar sebagai media penyimpanan. Gambar baboon, lena, Lichtenstein, monarch dan yatch diambil dari Astuti dkk [1] sedangkan gambar sport center diambil dari Alamsyah [1] seperti pada Gambar 2 berikut.



Gambar 2. Dataset eksperimen

3.1 Alur Eksperimen

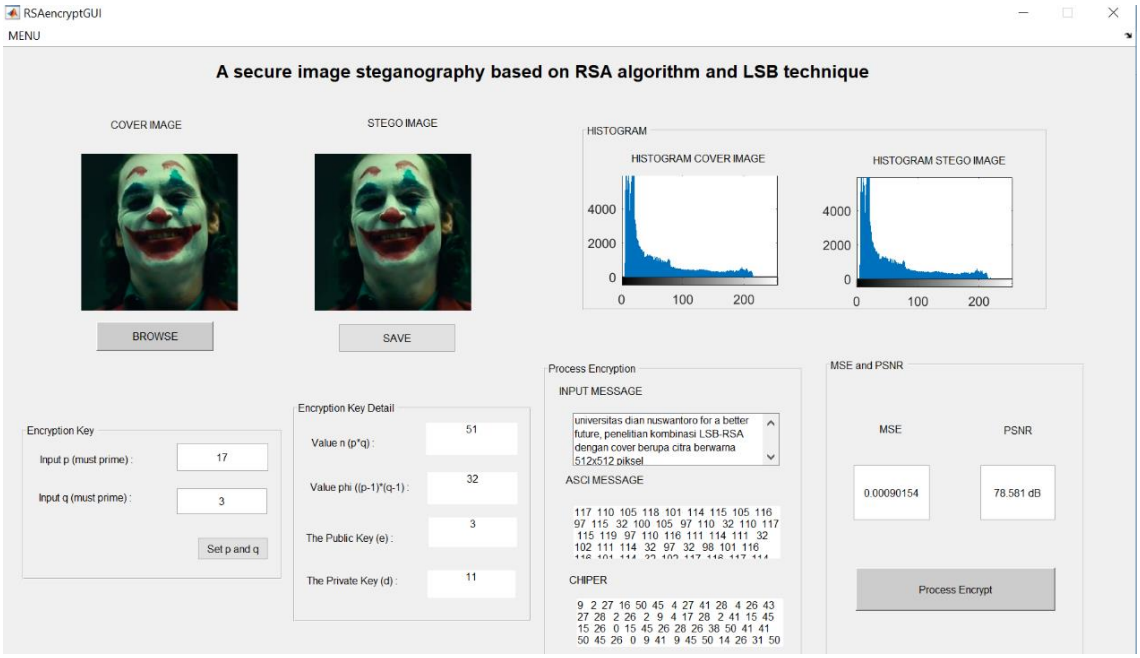
Pada bagian ini akan dijelaskan alur eksperimen menggunakan cover gambar 512x512 piksel sedangkan pesan berupa teks dengan panjang sesuai inputan (dapat diinputkan dengan maksimal *payload* sesuai ukuran gambar cover) seperti pada Gambar 2. Pada makalah ini, telah dibuat aplikasi implementasi LSB-RSA menggunakan matlab dalam bentuk *Graphical User Interface (GUI)* sehingga alur eksperimen lebih mufah untuk dipahami.



Gambar 3. Alur Eksperimen LSB-RSA

4. HASIL DAN PEMBAHASAN

Langkah pertama implementasi adalah membuat coding kombinasi yang kemudian dipaparkan dalam bentuk GUI seperti pada Gambar 3.



Gambar 4. GUI hasil implementasi LSB-RSA

Tabel 1. Perbandingan hasil PSNR pada beberapa penelitian terkait dengan gambar

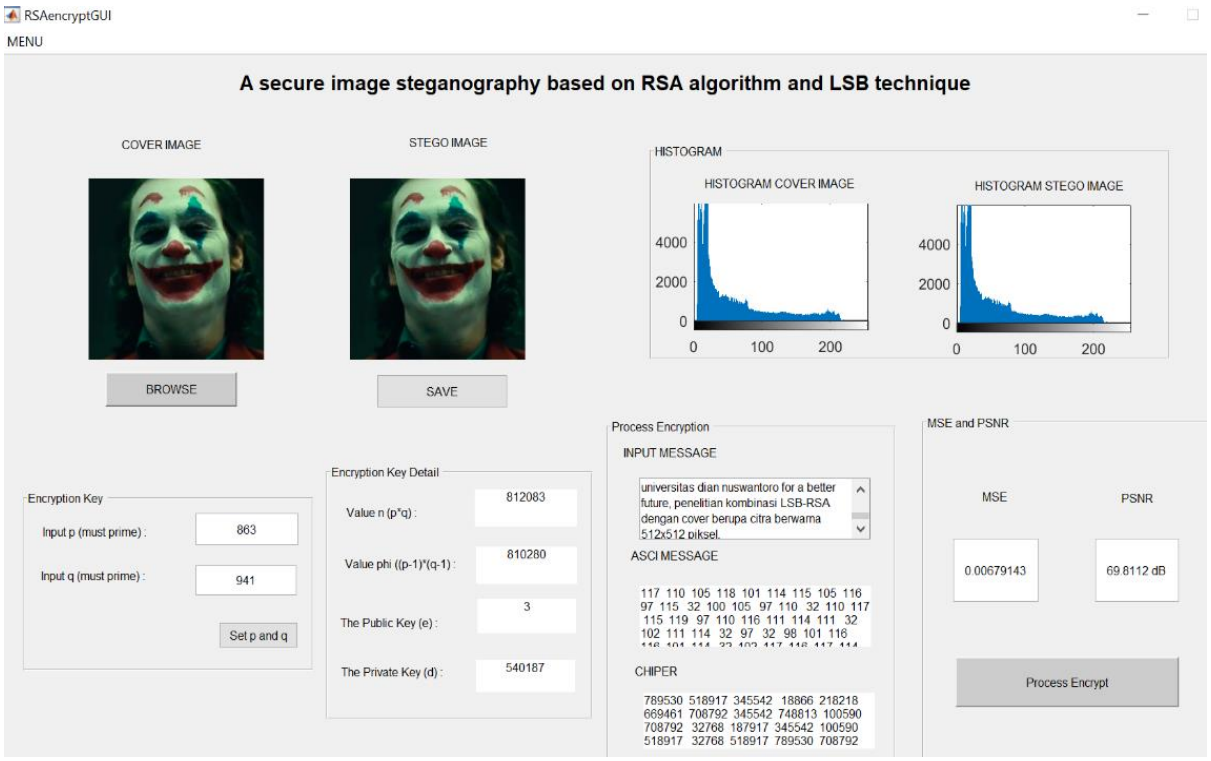
Metode	Astuti dkk [1]	Astuti dkk [1]	Usulan metode
Ukuran gambar Cover	512x512	512x512	512x512
Jenis gambar Cover	grayscale	RGB	RGB
Jenis Pesan	biner	RGB	Teks
Ukuran Pesan	32x32	256x128	1024 bit
Metode	LSB dan XOR MSB	LSB Flipping bit	LSB-RSA
PSNR	69 dB	56 dB	78.5383 dB

Berdasarkan Tabel 1, diketahui bahwa nilai PSNR pada makalah ini lebih tinggi dibanding dengan penelitian yang dilakukan olehh Astuti dkk [1] dan Astuti dkk [1]. PSNR sebesar 78.5383 dB pada gambar jocker.bmp diperoleh melalui eksperimen dengan inputan nilai p = 17, q = 3, publik key = 3 dan privat key = 11. Diketahui bahwa nilai PSNR akan berubah apabila inputan pesan teks ditambah. Berikut hasil percobaan yang telah di lakukan sesuai pada Tabel 2.

Tabel 2. Perbandingan Nilai PSNR dalam beberapa ukuran pesan teks

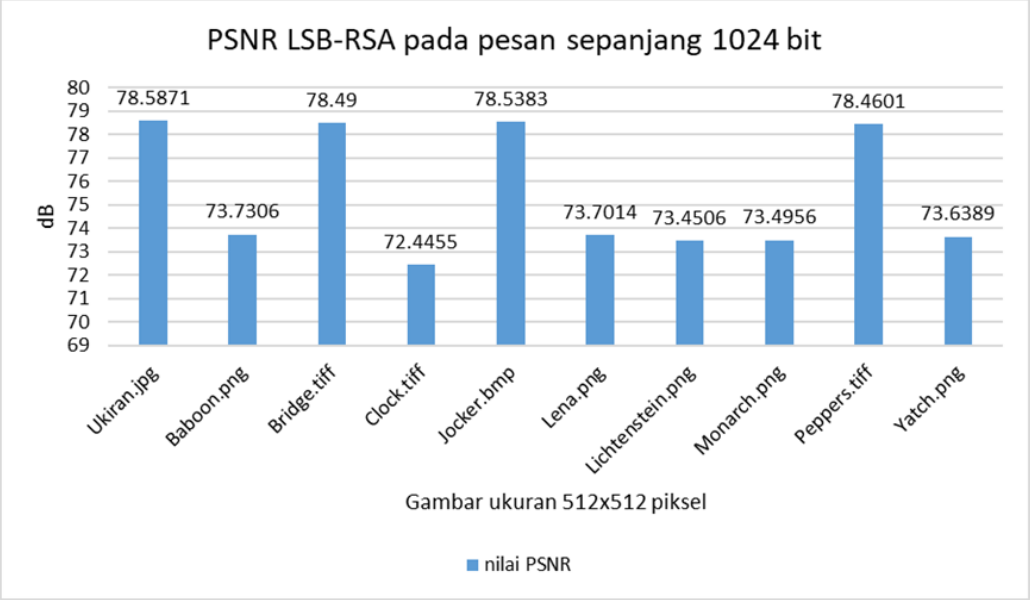
Nilai p	Nilai q	Publik key	Privat key	Teks	PSNR
17	3	3	11	universitas dian nuswantoro for a better future, penelitian kombinasi LSB-RSA dengan cover berupa gambar berwarna 512x512 piksel (1024bit)	78.5383 dB
17	3	3	11	universitas dian nuswantoro for a better future, penelitian kombinasi LSB-RSA dengan cover berupa citra berwarna 512x512 piksel universitas dian nuswantoro for a better future, penelitian kombinasi LSB-RSA dengan cover berupa citra berwarna 512x512 piksel universitas dian nuswantoro for a better future, penelitian kombinasi LSB-RSA dengan cover berupa citra berwarna 512x512 piksel. (3072 bit)	73.8446 dB
89	79	5	1373	universitas dian nuswantoro for a better future, penelitian kombinasi LSB-RSA dengan cover berupa citra berwarna 512x512 piksel (1024 bit)	76.1044 dB
863	941	3	540187	universitas dian nuswantoro for a better future, penelitian kombinasi LSB-RSA dengan cover berupa citra berwarna 512x512 piksel (1024 bit)	74.6521 dB
863	941	3	540187	universitas dian nuswantoro for a better future, penelitian kombinasi LSB-RSA dengan cover berupa citra berwarna 512x512 piksel universitas dian nuswantoro for a better future, penelitian kombinasi LSB-RSA dengan cover berupa citra berwarna 512x512 piksel universitas dian nuswantoro for a better future, penelitian kombinasi LSB-RSA dengan cover berupa citra berwarna 512x512 piksel. (3072 bit)	69.8112 dB

Menurut Tabel 2, dapat disimpulkan bahwa nilai p dan q yang besar sedikit mempengaruhi nilai PSNR, dimana terjadi sedikit penurunan nilai. Penggunaan teks dengan jumlah 1024 bit dan 3072 bit juga berpengaruh pada penurunan PSNR, namun tidak signifikan. Perolehan nilai PSNR dengan maksimum *payload* masih menghasilkan PSNR terendah 69 dB. Percobaan juga menggunakan histogram sebagai alat uji seperti pada Gambar 4, sedangkan pada Gambar 5 akan dipaparkan peroleh nilai PSNR pada seluruh dataset yang di uji menggunakan pesan teks 1024 bit seperti pada Tabel 2 di atas.



Gambar 5. Hasil implementasi dengan maksimum *payload* 3072 bit beserta tampilan histogram hasil stegano

Berbagai tipe gambar yaitu bmp, jpg, tiff, dan png telah diuji coba sesuai pada Gambar 6 berikut menggunakan nilai p = 17 dan q = 3.



Gambar 6. Hasil implementasi LSB-RSA pada dataset dengan pesan sepanjang 1024 bit

Bedasarkan Gambar 5 dan Gambar 6, telah dibuktikan performa dari LSB-RSA yang telah dibandingkan dengan dua buah penelitian terdahulu milik Astuti dkk [1] dan Astuti dkk [1]. Penelitian Astuti dkk dengan cover 512x512 grayscale dan pesan biner menghasilkan 69 dB, peroleh nilai cukup tinggi namun masih menggunakan pesan berupa gambar biner dengan ukuuran yang kecil yaitu 32x32 bit. Penelitian lain oleh Astuti dkk [1] menggunakan LSB flipping bit menghasilkan PSNR jauh lebih rendah, hal ini dapat terjadi karena penggunaan berupa pesan berwarna berukuran 256x128 dan menghasilkan PSNR 56 dB. Sedangkan dalam makalah ini LSB dikombinasi dengan RSA pada cover gambar 512x512 gambar berwarna dengan pesan teks pada maksimum payload yaitu 3072 bit dan mendapatkan PSNR sebesar 69.8112 dB pada nilai p dan q mendekati 1000.

5. KESIMPULAN

Pada penelitian ini, telah diterapkan metode LSB-RSA pada gambar 512x512 piksel dengan cover berupa gambar berwarna dan pesan berupa teks dengan panjang 1024 bit sampai 3072 bit. PSNR yang dihasilkan hampir mendekati 80 dB untuk pesan 2014 bit dan 69 dB untuk pesan 3072 bit. Dilihat dari histogram, gambar asli dan gambar hasil proses LSB tidak berbeda. Berdasarkan perbandingan yang dilakukan pada dua buah penelitian terkait, dapat disimpulkan hasil PSNR yang diperoleh lebih tinggi dari kedua penelitian terdahulu. Perubahan nilai PSNR bergantung pada nilai p dan q yang dipilih, apabila p dan q besar maka nilai kunci privat yang dihasilkan juga besar.

DAFTAR PUSTAKA

[1] Antonius Erick Handoyo, D.R.I.M. Setiadi, Eko Hari Rachmawanto, and Christy Atika Sari, "Teknik Penyembunyian dan Enkripsi Pesan pada Citra Digital dengan Kombinasi Metode LSB dan RSA," *Jurnal Teknologi dan Sistem Komputer*, vol. 6, no. 1, pp. 37-43, 2018.

[2] Eko Hari Rachmawanto, Rofi' Syaiful Amin, D.R.I.M. Setiadi, and Christy Atika Sari, "A performance analysis StegoCrypt algorithm based on LSB-AES 128 bit in various image size," , Semarang, 2017.

[3] Edi Jaya Kusuma, Oktaviana Rena Indriani, Christy Atika Sari, Eko Hari Rachamwanto, and D.R.I.M Setiadi, "Imperceptible LSB Image Hiding on Edge Region Using DES Encryption," in *International Conference on Innovative and Creative Information Technology (ICItech)*, Salatiga, 2018.

[4] Nadeem Akhtar, Pragati Johri, and Shahbaaz Khan, "Enhancing the Security and Quality of LSB based Image Steganography," in *International Conference on Computational Intelligence and Communication Networks*, 2013.

[5] M.F. Alamsyah. (2015) Implementasi metode Steganografi Least Significant bit dengan Algoritma RSA pada citra BMP.

[6] Yani Parti Astuti, D.R.I.M. Setiadi, Eko Hari Rachmawanto, and Christy Atika Sari, "Simple and Secure Image Steganography using LSB and Triple XOR Operation on MSB," in *International Conference on Information and Communications Technology (ICOIACT)*, Yogyakarta, 2018.

[7] Erna Zuni Astuti, D.R.I.M. Setiadi, Eko Hari Rachmawanto, Christy Atika Sari, and Md Kamruzzaman Sarker, "LSB-based Bit Flipping Methods for Color Image Steganography," in *ICERA 2019*, Yogyakarta, 2019.

[8] Candra Irawan, D.R.I.M Setiadi, Christy Atika Sari, and Eko Hari Rachmawanto, "Hiding and Securing Message on Edge Areas of Image using LSB Steganography and OTP Encryption ," , Semarang, 2017.

[9] Cahaya Jatmoko, Lekso Budi Handoko, Christy Atika Sari, and D.R.I.M Setiadi, "Uji Performa Penyisipan Pesan Dengan Metode LSB dan MSB Pada Citra Digital Untuk Keamanan Komunikasi," *Dinamika Rekayasa*, pp. 47-58, 2018.

[10] Mohammed Abdul Majeed and Rossilawati Sulaiman, "An Improved LSB Image Steganography Technique Using Bit Inverse in 24 bit Colour Image," *Journal of Theoretical and Applied Information Technology*, vol. 80, no. 2, pp. 342-348, 2015.

[11] Edi Jaya Kusuma, Christy Atika Sari, Eko Hari Rachmawanto, and D.R.I.M Setiadi, "A Combination of Inverted LSB, RSA, and Arnold Transformation to get Secure and Imperceptible Image Steganography ," *J. ICT Res. Appl*, vol. 12, no. 2, pp. 103-122, 2018.

[12] P Malathi and T. Gireeshkumar, "Relating the embedding efficiency of LSB Steganography techniques in Spatial and Transform domains," *Procedia Computer Science*, vol. 93, pp. 878 – 885, 2016.